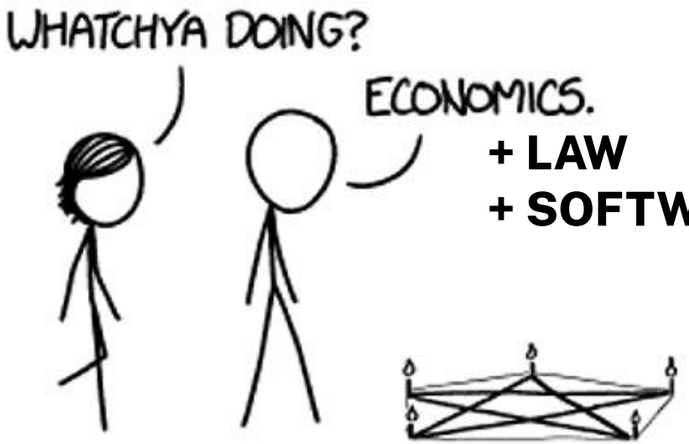
Lemons and Liability
Cyber Warranties as an Experiment in Software Regulation

Daniel W Woods

Coalition

THE UNIVERSITY of EDINBURGH

What to expect from this talk



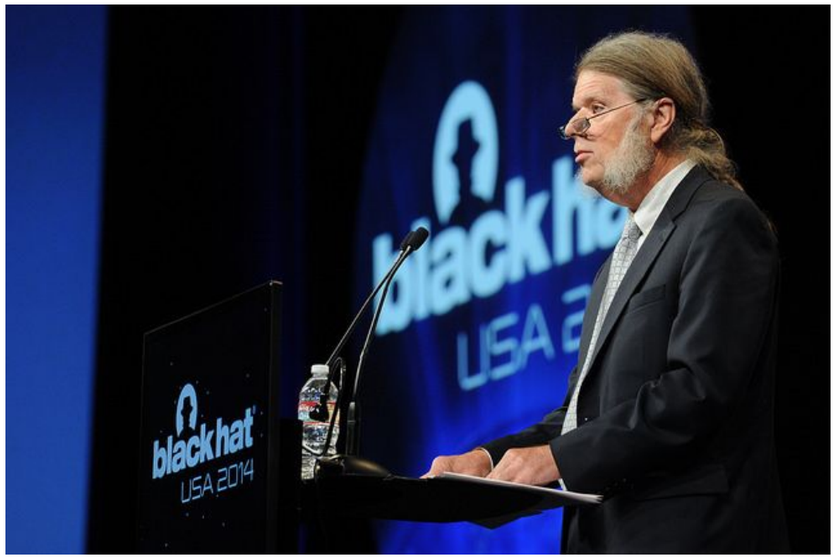
+ LAW
+ SOFTWARE SECURITY

Source: xkcd

Agenda

1. Convince you that **software liability is important**
2. Tell you a **story about cyber warranties**
3. Collect your esteemed perspectives on **how to design a safe harbor**

“the only two products not covered by product liability today are **religion** and **software**”



[Cybersecurity as Realpolitik (27:08)]

Software security as a lemons market

cost $200k — security reviews throughout dev lifecycle, bug bounty program etc

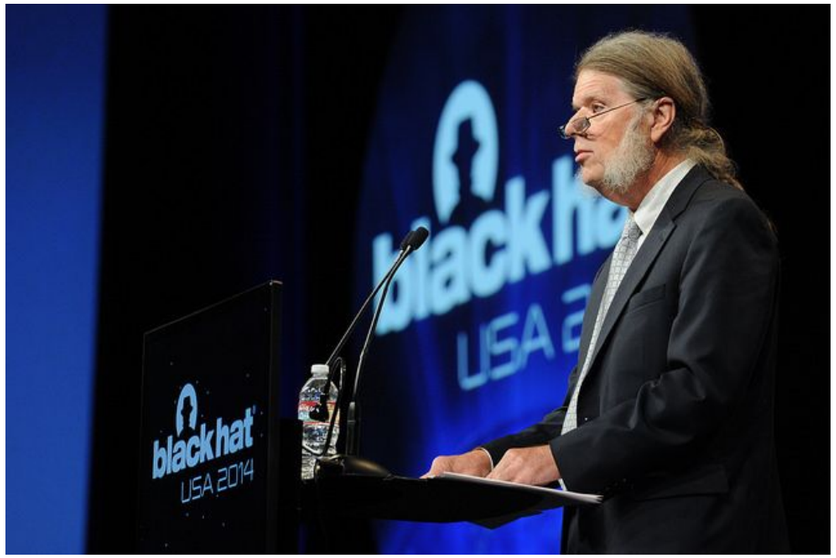
cost $100k — none of the above

If the buyer cannot identify insecure software, do they buy  or  ?

Akerlof, 1970. The Market for "Lemons": Quality Uncertainty and the Market Mechanism, *The Quarterly Journal of Economics*, Oxford University Press, vol. 84(3), pages 488-500

How can we incentivize vendors to build 🍑s instead of 🍋s?

"the only two products not covered by product liability today are **religion** and **software**, and software should not escape for much longer"



Cybersecurity as Realpolitik (27:08)

If the vendor is liable for $1m for any security breach, does the vendor build

 **or**  **?**

The right amount of software liability

No liability

Optimal liability

No innovation

Stricter liability regime

"We must begin to **shift liability** onto those entities that **fail to take reasonable precautions** to secure their software "

https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

A safe harbor protects vendors from liability

Safe harbor in the context of software liability

Vendors are **immune from liability** if they implement:

1. Secure software development process A
2. Secure software development process B

…

N. Secure software development process X

Agenda

2. Tell you a **story about cyber warranties**

The first cyber warranty

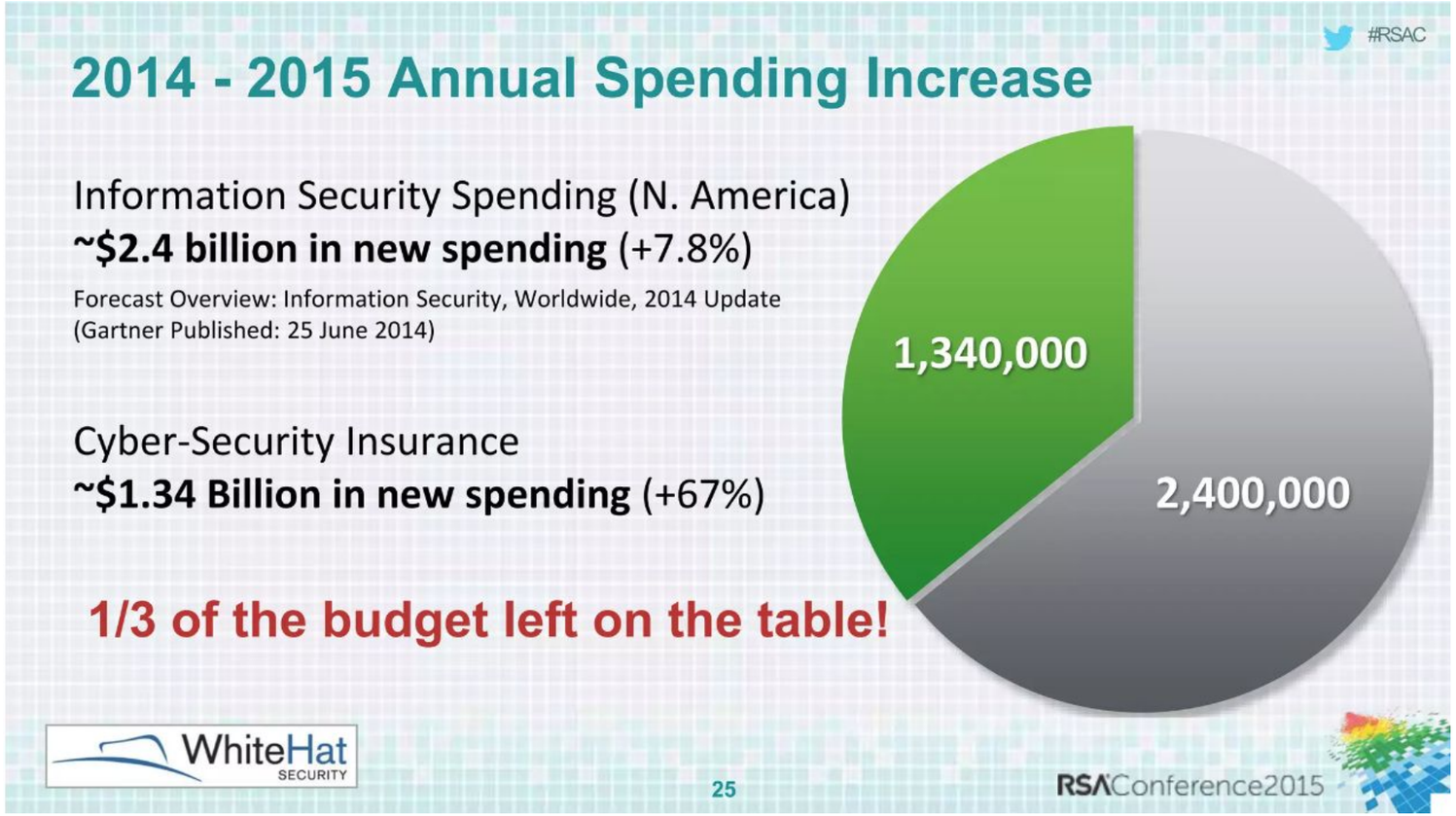
Black Hat USA 2014

Jeremiah Grossman announces that WhiteHat **will pay up to $250k** in breach related costs to any* customer that is hacked

RSA 2015

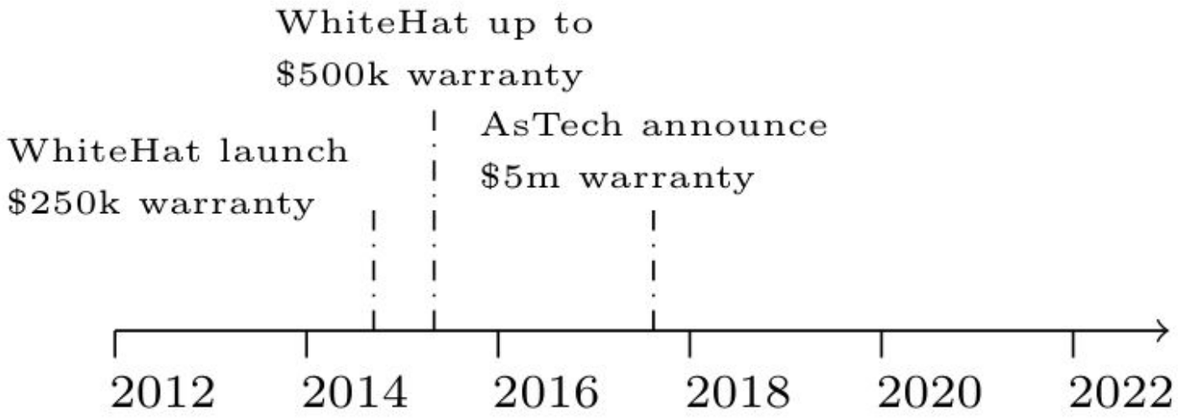
Limit upped to $500k and he talks about emerging insurance market

***T&Cs apply**



No More Snake Oil: Why InfoSec Needs Security Guarantees

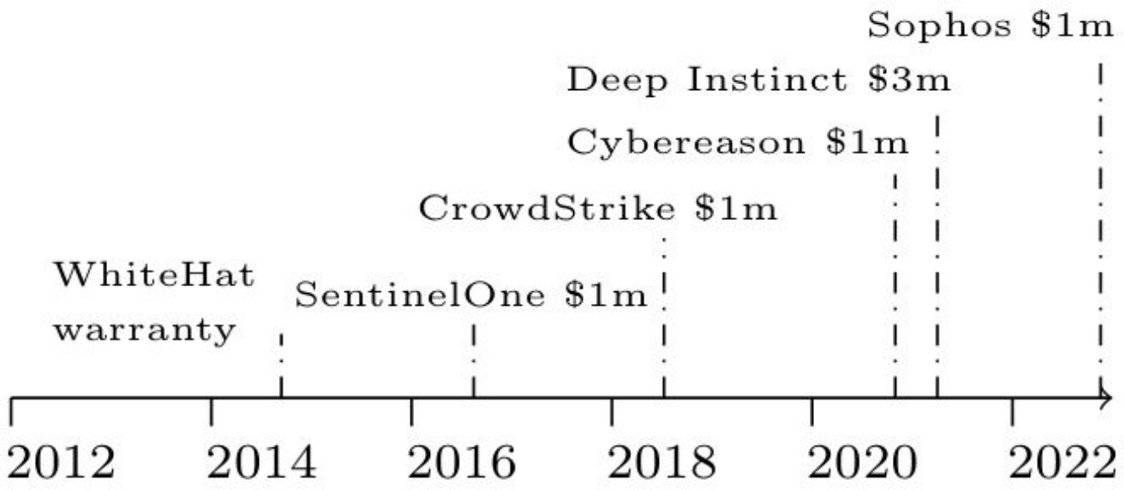
Competitors do not offer warranties



Gartner's Application Security Testing Market (as of 2023):

Vendor	Rating	Reviews
Veracode (Verracode)	4.7	304
Checkmark (SAST)	4.5	282
Rapid7 (InsightAppSec)	4.3	189
Port Swigger (Burp Suite Pro)	4.8	186
Qualys (Web App Scanning)	4.3	164
Invicti (Acunetix)	4.6	142
Synopsys (WhiteHat DAST)	**4.5**	**142**
Contrast Security (Security Platform)	4.6	137
... (No AsTech)		

Vendors get religion



Gartner's Endpoint Protection Platforms (EPP) Market:

Vendor (Product)	Rating	Reviews
Trellix (Endpoint Security)	4.5	1598
Symantec (Endpoint Protection)	4.4	1568
Microsoft (Defender)	4.4	1307
Sophos (Intercept X)	**4.8**	**1118**
Trend Micro (Apex One)	4.6	1052
SentinelOne (Singularity)	**4.8**	**949**
CrowdStrike (Falcon)	**4.8**	**846**
Malwarebytes (Endpoint Protection)	4.6	678
Cylance (PROTECT)	4.6	508
VMware (Carbon Black Cloud)	4.6	357

Vendors offering warranties as of Q1 2023*

Vendor	Rating	Year	Limit
WhiteHat Security	Security audit	2015	$500k
SentinelOne	End-point	2016	$1m
MyDigitalShield	Network	2016	$50k
Cymmetria	Deception	2016	$1m
AsTech	Security audit	2017	$5m
CrowdStrike	End-point	2018	$1m
Cybereason	End-point	2020	$1m
ThreatAdvice	MSP	2020	$250k
Deep Instinct	End-point	2021	$3m
Rubrik	Back-up	2021	$5m
Arctic Wolf	SOC	2021	$1m
Sophos	End-point	2022	$1m
Kroll	End-point	2022	$1m
Veam	Back-up	2023	$5m

*Let me know if I missed any!

Do cyber warranties solve the **lemons market**?

Criticisms of warranties

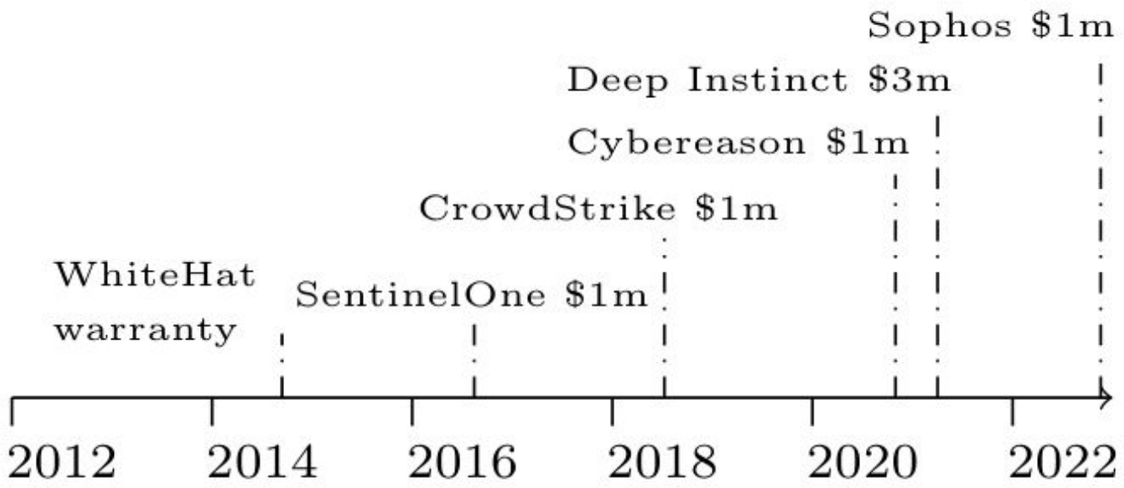
Objection 1
Better ways to spend, such as improving security

Objection 2
Warranties are sales tricks, T&Cs always apply

Objection 1: Better ways to spend money

Answer: Cyber warranties are **costly signals** designed to escape the lemons market.

Warranties as a quality signal



Cyber warranties are offered alongside **23% of all end-point protection products** for which Gartner collect ratings.

Buyers report **higher satisfaction** with cyber warrantied EPP products (**4.81 vs 4.46**).

Objection 2: Cyber warranties are sales tricks!

Answer: It depends on the specifics of the T&Cs

Yes

Liability limits can be **deceptive**:

- $5m limit falls to $250k if customer holds 500 terrabytes or less of data
- EDR vendors often limit liability to a max of $1k per machine

No

There are no silver bullets for security

- App testing firm's warranty only covers CVEs known at time of audit
  - **0-days not covered**
- End-point warranties typically require configuration and maintenance

Customer **must follow the [Vendor's] security best practices** …
includes the following:

Data Encryption
• Data-at-rest and in-transit are ***always encrypted***
• ***Secure protocols*** for third-party systems

Application Access
• Create ***IP whitelisting*** that limits connections to Customer owned networks only
• ***SSL-certificate security*** for User Interface (UI) and APIs

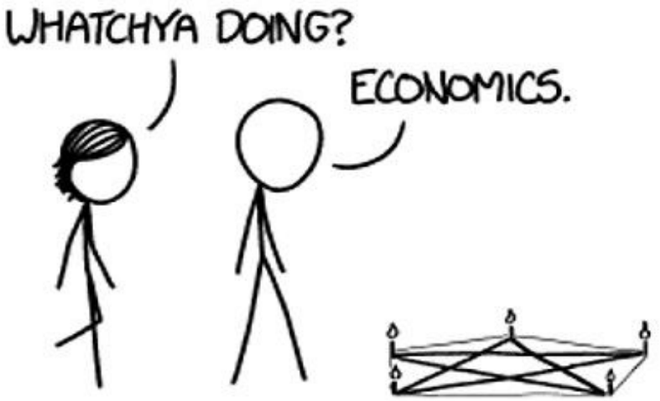
API Security
• ***Secure service accounts***
• Scoped ***API roles with least privilege***

Data Health
• ***Back-ups are successful*** and meet the SLA Policies
• Retention lock is enabled for the ***Customer data*** in the SLA Policies

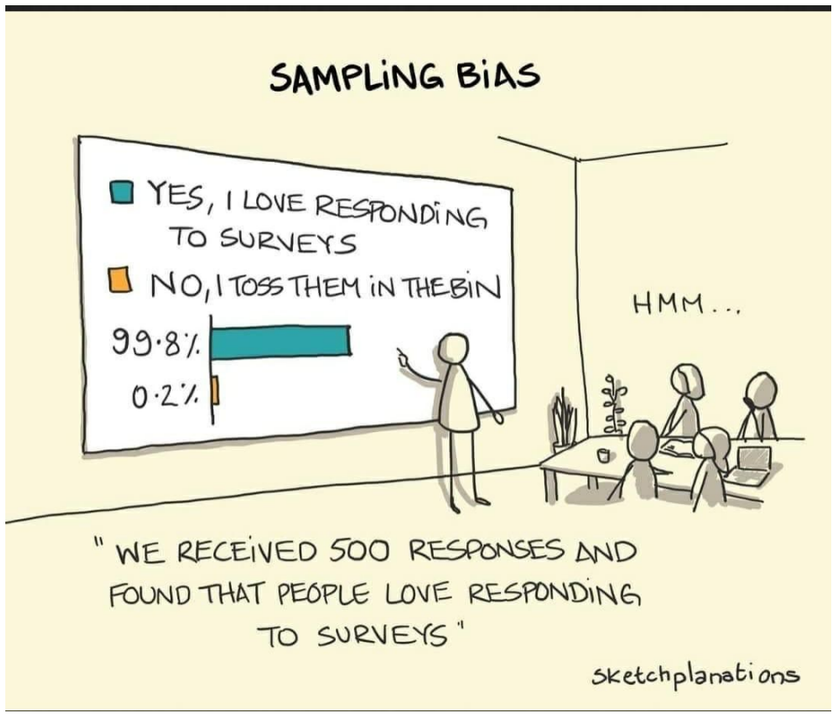
User Access
• ***Multi-factor authentication*** for all user accounts
• SSH key-based with ***passphrase protected keys*** for CLI authentication
• User roles are assigned with ***least privilege access***

Cyber warranties cliff notes

- Since the first warranty at BlackHat 2024, an extra **15 cyber warranties have been announced**
- **23% of EPP products** now offered with a warranty
- Warranties **signal effectiveness** of InfoSec products
- Pay attention to **terms and conditions**
  - Some sales tricks
  - Some incentives for better security



Agenda



3. Collect your esteemed perspectives on **how to design a safe harbor**

What is the **design space** in this context?

Broad options

higher level, less specific

List of measures that qualify vendor for safe harbour

Frameworks a vendor must follow to qualify for safe harbour

Guiding principles that vendors must follow

Safe harbor vs reverse safe harbor

Not liable if you do:

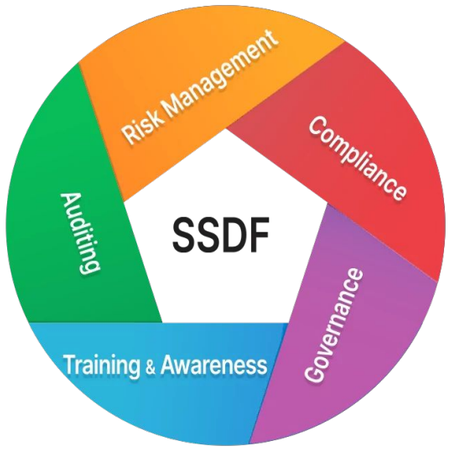
1. Good practice 1
2. Good practice 2
3. …

Become liable if you do:

1. Bad practice 1
2. Bad practice 2
3. …

Idea from Derek Bambauer

Which areas of security?



Appsec and/or **Infosec**

One vs many safe harbors

Online gaming

Healthcare

Stricter liability regime

What about **open source** software ?

Untangling root causes
in complex systems?

Legal evidence?

Key takeaways

Liability pushes vendors to secure software

Vendors are increasingly liable for security failures

Cyber warranties achieve higher customer satisfaction

Designing the safe harbor is an important technical problem

Thank you!

Please share the survey with relevant colleagues and reach out to share your ideas and experiences.

Contact details

daniel.woods@ed.ac.uk
daniel.woods@coalitioninc.com

https://www.danielwoods.info/

BIG QR CODE THAT LINKS TO THE SURVEY

(on day of presentation)

Coalition

THE UNIVERSITY of EDINBURGH